Two-Element Generation of Unitary Groups over Finite Fields

by

Bradley Scott Sears

Bachelor of Science, Indiana University

Master of Science, Central Missouri State University

A Dissertation Submitted in Partial Fulfillment
of the Requirements for the Doctor of Philosophy Degree

Department of Mathematics in the Graduate School
Southern Illinois University at Carbondale

June, 1999

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE 3.Nov.99	3. REPORT TYPE AND DATES COVERED DISSERTATION

4. TITLE AND SUBTITLE TWO-ELEMENT GENERATION OF UNITARY GROUPS OVER FINITE FIELDS	5. FUNDING NUMBERS
6. AUTHOR(S) CAPT SEARS BRADLEY S	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) SOUTHERN ILLINOIS UNIVERSITY AT CARBONDALE	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) THE DEPARTMENT OF THE AIR FORCE AFIT/CIA, BLDG 125 2950 P STREET WPAFB OH 45433	10. SPONSORING/MONITORING AGENCY REPORT NUMBER FY99-402

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION AVAILABILITY STATEMENT Unlimited distribution In Accordance With AFI 35-205/AFIT Sup 1	12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

DISTRIBUTION STATEMENT A
Approved for Public Release
Distribution Unlimited

19991117 071

14. SUBJECT TERMS	15. NUMBER OF PAGES 38
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT

DTIC QUALITY INSPECTED 4

SIU

Dissertation Approval
The Graduate School
Southern Illinois University

May 28, 1999

I hereby recommend that the dissertation prepared under my supervision by

Bradley Scott Sears

Entitled

Two-Element Generation of
Unitary Groups over Finite Fields

be accepted in partial fulfillment of the requirements for the

DOCTOR OF PHILOSOPHY degree

Andrew G. Earnest
In Charge of Dissertation

Andrew G. Earnest
Head of Department

Recommendation concurred in

1. Andrew G. Earnest
2. Robert W. Fitzgerald
3. Michael C. Sullivan
4. Joseph L Yucas
5. Nicholson C Phillips

Committee
for the
Final Examination

An Abstract of the Dissertation of Doctor of Philosophy

Bradley Scott Sears, for the Doctor of Philosophy Degree in Mathematics, presented on May 28, 1999, at Southern Illinois University at Carbondale.

TITLE: Two-Element Generation of Unitary Groups over Finite Fields

MAJOR PROFESSOR: Andrew Earnest

ABSTRACT: Minimal sets of generators of the unitary groups of nonsingular $\lambda-$hermitian spaces over a finite field of odd characteristic are studied. All such unitary groups are shown to be generated by two elements.

ACKNOWLEGMENTS

I would, first, like to praise my Lord and Savior, Jesus Christ, for allowing me this opportunity to work on a Ph.D in mathematics, and for His sustaining grace, comfort, and inspiration which has guided me to the point where I am now.

I would also like to express my undying love for my wife, Carrie, my daughter, Lauren, and my son, Jordan. Without your sacrifices to allow me to study and your constant love and support, I surely would have failed.

Finally, I would like to convey my appreciation for the esteemed members of my committee, Doctors Earnest, Fitzgerald, Yucas, Sullivan, and Phillips. Thank you for your support, guidance, and encouragement in this endeavor. Particularly to the chair, Dr. Earnest, who made time in his very busy schedule for countless hours of work with me, I could never thank you enough for your patient guidance.

TABLE OF CONTENTS

Introduction

Let V be a nonsingular λ-hermitian space of dimension n over a field K and $U(V)$ the unitary group on V. Under the assumption that K is a finite field of characteristic different from 2 and V is isotropic, Ishibashi showed in [12] that $U(V)$ is generated by three elements. Further, in fact, he proved that when the unitary group $U(V)$ is the symplectic group $Sp(V)$, then $U(V)$ is generated by just two elements.

This result was first refined by the works of Earnest, Ishibashi, and others in [2] and [7]. There the case where $U(V)$ is the orthogonal group $O(V)$ was studied. The restrictions of isotropy and characteristic were removed, thus, showing that when $U(V) = O(V), U(V)$ is generated by two elements.

The purpose of this paper is to again refine Ishibashi's original result. The paper's main theorem will show that all unitary groups over finite fields of odd characteristic are generated by only two elements. The bulk of the work, here, is in removing the restriction of isotropy when V is a λ-hermitian space which is not a quadratic space and in showing that when $U(V) \neq O(V)$ and $U(V) \neq Sp(V), U(V)$ is generated by two elements. The proof of this main result occurs in Chapter 4.

Prior to that, however, Chapter 1 will establish some key ideas about the underlying finite field. It defines the concept of an involution on a field, establishes the surjectivity of the norm and trace maps, and defines some naturally occurring subsets of the field.

Next, Chapter 2 will detail what a $\lambda-$hermitian space is and define the special cases of $\lambda-$hermitian spaces. Chapter 2 also discusses classification of these spaces and the property of isotropy. Chapter 2 is where one sees the ability to remove the restriction of isotropy from nonquadratic $\lambda-$hermitian spaces.

Finally, Chapter 3 develops the idea of the unitary groups over $\lambda-$hermitian spaces. The generating maps used in the main theorem will be defined along with some essential identities for combining them.

Chapter 1

The Underlying Field

Throughout this chapter, all fields under consideration will be assumed to be finite. Moreover, for the entirety of this paper, all fields will be assumed to have odd characteristic. The theory which will be developed herein is fundamentally different for finite fields of characteristic two and therefore will not be treated at this time.

Consequently, the underlying field K considered here has order $q = p^m$ for some odd prime p and natural number m. The multiplicative group $\dot{K} = K \backslash \{0\}$ is well known to be a cyclic group. Here and throughout the remainder of this paper, α will denote a fixed generator of this group; that is, $\dot{K} = \langle \alpha \rangle$.

1. Some Important Maps of the Underlying Finite Field.

Let F be a subfield of K. Then K is known to be a finite Galois extension of F. Let $Aut_F K = \{\sigma_1, \ldots, \sigma_n\}$ be the Galois group of K over F. In fact, $Aut_F K$ is a cyclic group generated by the Fröbenius automorphism σ defined by $\sigma(a) = a^\ell$ for $a \in K$, where $\ell = |F|$.

The first two maps to be defined and discussed are the norm and trace maps of the extension K/F. It will be shown that these maps are surjective in the present context.

1.1.1 Definition. *The norm map of K/F is defined as $N[K/F](k) = \sigma_1(k)\sigma_2(k)\ldots\sigma_n(k)$ for $k \in K$.*

1.1.2 Definition. *The trace map of K/F is defined as $T[K/F](k) = \sigma_1(k) + \sigma_2(k) + \cdots + \sigma_n(k)$ for $k \in K$.*

Most of the time, the norm and trace of an element $k \in K$ will be denoted $N(k)$ and $T(k)$ since the fields over which they are defined will be obvious to discern.

1.1.3 Lemma. *The norm $N[K|F]$ is surjective.*

Proof. Now, $N[K/F](\alpha) = N(\alpha) = \alpha\alpha^{\ell}\alpha^{\ell^2}\dots\alpha^{\ell^{(n-1)}} = \alpha^{\ell^n-1/\ell-1}$. But this implies that $(N(\alpha))^{\ell-1} = \alpha^{\ell^n-1} = 1$. What is more is that this is the smallest such power. For if there were a smaller power s for which $(N(\alpha))^s = 1$, then $\left(\alpha^{\frac{\ell^n-1}{\ell-1}}\right)^s = \alpha^{\frac{\ell^n-1}{t}} = \alpha^{\ell^n-1/t}$ where $\ell - 1 = st$, $t \in \mathbb{N}$ and $\alpha^{\ell^n-1/t} = 1$. This, of course, cannot happen since $\dot{K}$ is generated by α and has order $\ell^n - 1$. Hence, $N(\alpha)$ has order $\ell - 1$.

Note, however, that $N(\dot{K}) = \langle N(\alpha)\rangle$ since $\dot{K} = \langle\alpha\rangle$. Thus, $|N(\dot{K})| = \ell - 1$. Also, $|\dot{F}| = \ell - 1$. Hence, $|N(\dot{K})| = |\dot{F}|$. Therefore, $N[K/F]$ is surjective. □

1.1.4 Lemma. *The trace $T[K/F]$ is surjective.*

Proof. It suffices to show that 1_F has a pre-image in K, since 1_F generates F additively. Now, by Dedekind's theorem on the independence of characters, $\{\sigma_1, \sigma_2, \dots, \sigma_n\}$ is linearly dependent over K. Thus, there exists $\delta \in K$ such that $\sigma_1(\delta) + \sigma_2(\delta) + \cdots + \sigma_n(\delta)$ does not equal zero. But this is $T[K/F](\delta) = T(\delta)$. Hence, $T\left(\frac{1}{T(\delta)}\delta\right) = \frac{1}{T(\delta)}T(\delta) = 1_F$. Therefore, the trace is surjective. □

These two surjections will prove to be invaluable in establishing important facts about hermitian spaces and their unitary groups in the next two chapters.

Finally, the concept of an involution of the finite field K must be set forth.

1.1.5 Definition. *An involution of the finite field K is an antiautomorphism* * *of K of order* ≤ 2.

Thus, $(a+b)^* = a^* + b^*, (ab)^* = b^*a^*, 1^* = 1$ and $(a^*)^* = a$ for $a, b \in K$. One observes immediately that the concept of an antiautomorphism of K is mute since K is a field and has commutative multiplication. Hence, $(ab)^* = b^*a^* = a^*b^*$. Also, the identity map over K is trivially an involution. However, it will be involutions which are different from the identity map which will be of primary interest. Further if it is assumed that the involution * fixes F in this case, then this map sending a to a^* for $a \in K$ is an element of order two in the Galois group $Aut_F K$. Thus, the fixed field of * is a subfield of index two in K. This idea will be revisited later.

2. Special Subsets of the Underlying Finite Field.

Let K be an arbitrary finite field of odd characteristic. Let $\alpha \in K$ be a fixed generator of the mulltiplicative cyclic group $\dot{K}$. First, consider the subset of elements in K consisting of the squares of nonzero elements of K. This set is denoted $\dot{K}^2$.

1.2.1 Definition. $\dot{K}^2 = \{k \ \in K \mid k = b^2$ *for some* $b \in \dot{K}\}$.

It is well known that $\dot{K}^2$ has exactly $\frac{1}{2}|\dot{K}|$ elements [17]. With this in mind, one can see that these elements are precisely the even powers of α.

1.2.2 Lemma. $\dot{K}^2 = \{\alpha^{2k} \mid k = 1, 2, \ldots, \frac{1}{2}|\dot{K}\ |\ \}$.

Proof. Let $S = \{\alpha^{2k} \mid k = 1, 2, \ldots, \frac{1}{2}|\dot{K}|\}$. Clearly, $S \subseteq \dot{K}^2$, since for any k, $\alpha^{2k} = (\alpha^k)^2$. One also notes from its definition that $|S| = \frac{1}{2}|\dot{K}|$. Thus, S is a subset of $\dot{K}^2$ which contains the same number of elements as $\dot{K}^2$. Hence, $\dot{K}^2 = S$. □

Likewise, $\dot{K}\backslash\dot{K}^2$ is comprised of the odd powers of the generator α.

This leads to the consideration of two sets of differences which appear naturally in the development of the main theorem in Chapter 4. They are the two sets containing the differences of even and odd powers of α respectively.

1.2.3 Definition.

$$\begin{aligned}\mathcal{E}_K &= \{x - y \mid x = \alpha^r \text{and } y = \alpha^s, r, s \textit{ even integers}\}\\ &= \{x - y \mid x, y \in \dot{K}^2\}.\end{aligned}$$

1.2.4 Definition.

$$\begin{aligned}\mathcal{O}_K &= \{x - y \mid x = \alpha^r, y = \alpha^s, r, s \textit{ odd integers}\}\\ &= \{x - y \mid x, y \in \dot{K}\backslash\dot{K}^2\}.\end{aligned}$$

$\mathcal{E}_K$ is a set which is particularly interesting, not only because of the natural way in which it arises, but because this set often encompasses all of K. Clearly $0 \in \mathcal{E}_K$, since $x - x = 0\ \forall x \in \dot{K}^2$. The following lemma also shows that most of the elements of $\dot{K}$ are members of $\mathcal{E}_K$ as well.

1.2.5 Lemma. *Let $\delta \in \dot{K}$ such that $\delta \neq \pm 1$. Then $\delta \in \mathcal{E}_K$.*

Proof. Let $x = \frac{\delta+1}{2}, y = \frac{\delta-1}{2}$. Both x and y are elements of $\dot{K}$ since $\delta \neq \pm 1$ and K is not of characteristic two. Further, $x^2 - y^2 = \left(\frac{\delta+1}{2}\right)^2 - \left(\frac{\delta-1}{2}\right)^2 = \frac{1}{4}[(\delta^2 + 2\delta + 1) - (\delta^2 - 2\delta + 1)] = \frac{1}{4}[4\delta] = \delta$. □

So, $\mathcal{E}_K$ contains all of K with the possible exception of the elements ±1. In fact, one observes readily that if $K = \{-1, 0, 1\}$, then $\mathcal{E}_K = \mathcal{O}_K = \{0\}$. Thus, any finite field with only three elements will present a problem when working with $\mathcal{E}_K$. However, when $|K| > 3$, one sees that $\{\pm 1\} \subseteq \mathcal{E}_K$ or $\{\pm 1\} \subseteq \mathcal{O}_K$.

1.2.6 Lemma. *Let $|K| > 3$. Then $\{\pm 1\} \subseteq \mathcal{E}_K$ or $\{\pm 1\} \subseteq \mathcal{O}_K$.*

Proof. Let $|K| \geq 5$. It suffices to show the result for $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, the field of p elements, since any other field F of characteristic p contains a copy of $\mathbb{F}_p$. Namely, it contains $\{m1_F \mid m \in \mathbb{Z}\}$. So, no harm results in identifying $\mathbb{F}_p$ with this subfield of F.

Hence, $\{1, 2, 3, 4\} \subseteq \dot{K}$ since $|K| \geq 5$. One observes, also, that $1, 4 \in \dot{K}^2$ regardless of p since $1 = 1^2$ and $4 = 2^2$. Now, if $2 \in \dot{K}^2$, then $\{\pm 1\} \subseteq \mathcal{E}_K$ since $2 - 1 = 1$ and $1 - 2 = -1$. If $2 \in \dot{K} \backslash \dot{K}^2$ and $3 \in \dot{K}^2$, then $\{\pm 1\} \subseteq \mathcal{E}_K$ since $4 - 3 = 1$ and $3 - 4 = -1$. Finally, if $2, 3, \in \dot{K} \backslash \dot{K}^2$, then $\{\pm 1\} \subseteq \mathcal{O}_K$ since $3 - 2 = 1$ and $2 - 3 = -1$. □

From the previous discussion and Lemmas 1.2.5 and 1.2.6, one sees that either $\mathcal{E}_K = K$ or $\mathcal{E}_K = K \backslash \{\pm 1\}$ and $\{\pm 1\} \subseteq \mathcal{O}_K$.

Finally, another set which occurs naturally when developing the theory of unitary groups is a set denoted by C in the literature. This section will conclude with the set's definition and the determination of its relationship to the fixed field of the involution $*$. First, consider the fixed field K_0 of the involution $*$ on the finite field K.

1.2.7 Definition. $K_0 = \{k \in K \mid k^* = k\}$.

K_0 is indeed a subfield of K since $(a - b)^* = a^* - b^* = a - b$ and $(ab^{-1})^* = a^*(b^*)^{-1} = ab^{-1}$ for all $a, b \in K_0$. Let β be a fixed generator of the multiplicative cyclic group $\dot{K}_0$. Note also that $\beta \neq 1$ since $charK \neq 2$. As a matter of notation, the subset of any given set which is fixed by the involution $*$ will be denoted by the subscript zero. Further, as alluded to earlier, when one views K as an extension of the finite field K_0, then $[K : K_0] = 2$. It is also important to note here that if the involution * is different from the identity then * must be the unique Fröbenius automorphism, σ, which sends element a of K to a^{ℓ}, where $|K_0| = \ell$.

Moreover, in this context, $\dot{K}_0 \subseteq \dot{K}^2$.

Lemma 1.2.8. *Let K be a finite field with $* \neq 1$. Then $\dot{K}_0 \subseteq \dot{K}^2$.*

Proof. Let $\delta \in \dot{K}_0$. By definition, $\delta^* = \delta$. But $\delta^* = \delta^{\ell}$ where $|K_0| = \ell$ since $* \neq 1$. Thus, $\delta^{\ell} = \delta$ implying $\delta^{\ell-1} = 1$. Now, $\delta = \alpha^s$ for some natural number s since $\delta \in \dot{K}$ and $\dot{K} = \langle \alpha \rangle$. Hence, $\alpha^{s(\ell-1)} = 1$. This implies that $\ell^2 - 1$ divides $s(\ell - 1)$ since $o(\alpha) = \ell^2 - 1$. Therefore, $(\ell + 1)|s$. However, $\ell + 1$ is even since ℓ is odd. So s must be even. Whence, by Lemma 1.2.2, $\delta \in \dot{K}^2$ and $\dot{K}_0 \subseteq \dot{K}^2$. □

Next, let λ be an element of K such that $\lambda\lambda^* = 1$. It is this element which will give shape to the structure of the λ–hermitian space over K which will be discussed in the next chapter. The set C consists of the elements $x \in K$ such that $x = -\lambda x^*$. Equivalently;

1.2.9 Definition. $C = \{x \in K \mid x + \lambda x^* = 0\}$.

1.2.10 Lemma. *If $C \neq \{0\}$, then $C = cK_0$ for any $0 \neq c \in C$.*

Proof. Let $0 \neq c \in C$. Take any b in C. Since one has $c + \lambda c^* = 0$ and $b + \lambda b^* = 0$, it follows that $bc^{-1} = -\lambda b^*(-\lambda c^*)^{-1} = \lambda\lambda^{-1} b^*(c^*)^{-1} = b^*(c^{-1})^* = (bc^{-1})^*$. This means that $bc^{-1} \in K_0$, and so $C \subseteq cK_0$.

Let $ck \in cK_0$. $ck + \lambda(ck)^* = ck + \lambda c^* k^* = ck + \lambda c^* k$, since $k \in K_0$. Thus, $ck + \lambda(ck)^* = k(c + \lambda c^*) = k0 = 0$. Hence, $ck \in C$ and $C \subseteq cK_0$. Therefore, $C = cK_0$. □

Thus, one has $cK_0 = \{c\beta^i \mid i = 1, 2, \ldots, \ell - 1\} \cup \{0\}$. Lemma 1.2.10 coupled with what has been shown about the set $\mathcal{E}_K$ will be instrumental in showing the generation of the unitary group over a two dimensional hermitian space.

Chapter 2

λ-Hermitian Spaces and their Properties

This chapter addresses some of the essential properties of $\lambda-$hermitian spaces used in the study of unitary groups in Chapter 3 and in the discussion of the main theorem in Chapter 4. The chapter consists of three subsections. The first subsection defines a $\lambda-$hermitian space and details some important structural elements common to all $\lambda-$hermitian spaces. Next, the second subsection sets forth the notion of isotropic spaces and discusses some pertinent results for $\lambda-$hermitian spaces. Finally, the third subsection formalizes what is meant by isometric $\lambda-$hermitian spaces. The three special types of $\lambda-$hermitian spaces giving rise to unitary groups are defined. Discussion regarding classification of these special spaces up to isometry is also provided in this subsection.

1. $\lambda-$Hermitian Spaces.

Let V be an n-dimensional left vector space over a field K with involution $*$ as described in Chapter 1. Any further mention of the term vector space refers to this description. Note that the underlying field need not be finite to achieve the results of this subsection.

2.1.1 Definition. *A sesquilinear form on V is a mapping $f : V \times V \to K$ such that*

i) $f(x_1 + x_2, y) = f(x_1, y) + f(x_2, y)$ $\forall$ $x_1, x_2, y \in V$,

ii) $f(x, y_1 + y_2) = f(x, y_1) + f(x, y_2)$ $\forall$ $x, y_1, y_2 \in V$,

iii) $f(ax, y) = af(x, y)$ $\forall\, a \in K, x, y \in V$, *and*

iv) $f(x, by) = f(x, y)b^*$ $\forall\, b \in K, x, y \in V$.

2.1.2 Definition. *Let λ be a fixed element of K with $\lambda\lambda^* = 1$. A sesquilinear form f on V satisfying $f(x,y)^* = \lambda f(y,x)\ \forall\ x, y \in V$ is called a λ–hermitian form on V. In this case, (V,f) is called a λ–hermitian space.*

2.1.3 Definition. *Two vectors x, y in a λ–hermitian space (V,f) are orthogonal if $f(x,y) = 0$. Let (U,f) be a subspace of (V,f). Define the orthogonal complement of U in V to be $U^\perp = \{v \in V \mid f(v,u) = 0\ \forall\ u \in U\}$.*

Notice that the condition of orthogonality is always symmetric since $f(x,y) = 0$ implies $f(y,x) = \lambda^{-1}f(x,y)^* = \lambda^{-1}0^* = \lambda^{-1}0 = 0$.

2.1.4 Definition. *The radical of a λ–hermitian space (V,f) is rad $V = V^\perp$ $= \{v \in V \mid f(v,x) = 0\ \forall\ x \in V\}$.*

2.1.5 Definition. *A λ–hermitian space (V,f) is said to be nonsingular if and only if rad $V = \{0\}$.*

A λ-hermitian space (V,f) is nonsingular if and only if there is no vector in V other than 0 which is orthogonal to the whole space. From this point forward, all λ–hermitian spaces are assumed to be nonsingular. Notice that nonsingularity implies that for any nonzero vector x in V there is a nonzero vector y such that $f(x,y) = 1$. Directly from the definition, nonsingularity implies that there is $0 \neq z \in V$ such that $f(x,z) = \delta \neq 0$. Hence, let $y = (\delta^{-1})^*z$ and $f(x,y) = f(x,(\delta^{-1})^*z) = f(x,z)\delta^{-1} = \delta\delta^{-1} = 1$.

Further, if $\lambda \neq -1$ or $^* \neq 1$, there is a vector u in V such that $f(u,u) \neq 0$. To see this choose a vector x in V. If $f(x,x) \neq 0$, then let $u = x$. Otherwise, choose another vector y in V such that $f(x,y) = 1$. Again, if $f(y,y) \neq 0$, then let $u = y$. If $f(y,y) = 0$, then consider $\Gamma : \dot{K} \to \dot{K}$ defined by $\Gamma(\gamma) = \gamma^*\gamma^{-1}$ for $\gamma \in \dot{K}$. The map Γ is a multiplicative homomorphism, since for $\gamma_1, \gamma_2 \in \dot{K}, \Gamma(\gamma_1\gamma_2) =$

$(\gamma_1\gamma_2)^*(\gamma_1\gamma_2)^{-1} = \gamma_2^*\gamma_1^*\gamma_2^{-1}\gamma_1^{-1} = (\gamma_1^*\gamma_1^{-1})(\gamma_2^*\gamma_2^{-1}) = \Gamma(\gamma_1)\Gamma(\gamma_2)$. If $\lambda \neq -1$, then $-\lambda^* \neq 1$. This implies $\Gamma(\delta) = \delta^*\delta^{-1} = 1 \neq -\lambda^*$ for all $\delta \in K_0$. If $^* \neq 1$, then for $\delta \in \dot{K}\backslash\dot{C}, \delta + \lambda\delta^* \neq 0$. Thus, $-\lambda^* \neq \delta^*\delta^{-1} = \Gamma(\delta)$. So if $f(y,y) = 0$, then there is a $\delta \in \dot{K}$ such that $\delta^*\delta^{-1} \neq -\lambda^*$. Let $u = x + \delta y$ and $f(u,u) = f(x+\delta y, x+\delta y) = f(x,x) + \delta^* f(x,y) + \delta f(y,x) + \delta\delta^* f(y,y) = \delta^* + \lambda^*\delta \neq 0$.

2.1.6 Definition. *A basis $\mathcal{B} = \{v_1, v_2, \ldots, v_n\}$ for a $\lambda-$hermitian space (V,f) is called an* <u>*orthogonal*</u> *basis if $f(v_i, v_j) = 0$ for $i \neq j$.*

2.1.7 Proposition. *Let (V,f) be an $n-$dimensional $\lambda-$hermitian space over K with $\lambda \neq -1$ or $^* \neq 1$. Then V has an orthogonal basis.*

Proof. The proof proceeds by induction on the dimension n of V. The result is vacuously true for $n = 1$.

Suppose that there is an orthogonal basis for any $(n-1)-$dimensional $\lambda-$hermitian space over K with $\lambda \neq -1$ or $^* \neq 1$. Let (V,f) be a similarly described $n-$dimensional λ-hermitian space over K. Since $\lambda \neq -1$ or $^* \neq 1$, choose a basis $S_1 = \{u_1, u_2, \ldots, u_n\}$ of V so that $f(u_1,u_1) \neq 0$. Let $y_i = u_i - \frac{f(u_i,u_1)}{f(u_1,u_1)}u_1$ for $i = 2, \ldots, n$ and consider $W = span\{y_2, \ldots, y_n\}$. Note that W is an $(n-1)-$dimensional $\lambda-$hermitian space over K with $f(u_1, y_i) = 0$ for $i = 2, \ldots, n$. By the inductive hypothesis, W has an orthogonal basis, say $\{z_2, \ldots, z_n\}$. Therefore, $\{u_1, z_2, \ldots, z_n\}$ is an orthogonal basis of V. □

2.1.8 Definition. *Let (V,f) be a $\lambda-$hermitian space and let (U,f) and (W,f) be subspaces of (V,f). V is the* <u>*orthogonal sum*</u> *of U and W, denoted $V = U \perp W$, if*

i) $V = U \oplus W$, and

ii) $f(u,w) = 0 \;\forall\; u \in U,\; w \in W$.

2.1.9 Proposition. *Let (V, f) be a $\lambda-$hermitian space and let (U, f) be a nonsingular subspace of (V, f). Then $V = U \perp U^{\perp}$.*

Proof. For the proof, see [17; Theorem 7.1.4]. □

Also, for any basis $\mathcal{B}$ of a $\lambda-$hermitian space (V, f), one can associate to the form f a matrix with respect to $\mathcal{B}$.

2.1.10 Definition. *The matrix of f with respect to a basis $\mathcal{B}$, denoted $M_{\mathcal{B}}$ is $(f(v_i, v_j))$ $1 \leq i,\ j \leq n$.*

2.1.11 Proposition. *Let $\mathcal{B} = \{e_1, e_2, \cdots, e_n\}$ and $\mathcal{B}' = \{e'_1, e'_2, \cdots, e'_n\}$ be bases of a $\lambda-$hermitian space (V, f). Let $P = (p_{ij})$ be such that $e'_j = \sum_{i=1}^{n} p_{ij} e_i$. Then $M_{\mathcal{B}'} = P^t M_{\mathcal{B}} P^*$, where P^t denotes the transpose of P and $P^* = (p^*_{ij})$.*

Proof.

$$\begin{aligned}
(P^t M_{\mathcal{B}} P^*)_{ij} &= \sum_{h=1}^{n} \left(\sum_{k=1}^{n} p_{ki} f(e_k, e_h) \right) p^*_{hj} \\
&= \sum_{k=1}^{n} \sum_{h=1}^{n} p_{ki} p^*_{hj} f(e_k, e_h) \\
&= \sum_{k=1}^{n} p_{ki} \sum_{h=1}^{n} p^*_{hj} f(e_k, e_h) \\
&= \sum_{k=1}^{n} p_{ki} f \left(e_k, \sum_{h=1}^{n} p_{hj} e_h \right) \\
&= f \left(\sum_{k=1}^{n} p_{ki} e_k, \sum_{h=1}^{n} p_{hj} e_h \right) \\
&= f(e'_i, e'_j) \\
&= (M_{\mathcal{B}'})_{ij} \quad \square
\end{aligned}$$

Since (V, f) is nonsingular, there is a basis $\mathcal{B}$ of V with $det M_{\mathcal{B}} \neq 0$. Because of the change of basis formula in Proposition 2.1.11, one can easily see that for any other basis $\mathcal{B}'$ of V the matrix $M_{\mathcal{B}'}$ has a nonzero determinant as well. It follows then that a $\lambda-$hermitian space (V, f) is nonsingular if and only if $detM_B \neq 0$ for every basis B of V. More specifically, if $\lambda \neq -1$ and $^* \neq 1$, then the matrix associated to an orthogonal basis of V has a nonzero determinant implying for such a basis $B = \{e_1, e_2, \ldots, e_n\}$ that $f(e_i, e_i) \neq 0$ for $i = 1$ to n.

2. Isotropy of $\lambda-$Hermitian Spaces.

For the purposes of this subsection also, it is again the case that the underlying field need not be finite.

2.2.1 Definition. *For a $\lambda-$hermitian space (V, f), a nonzero vector $v \in V$ is said to be isotropic if $f(v, v) = 0$. Otherwise, v is anisotropic.*

2.2.2 Definition. *A $\lambda-$hermitian space (V, f) is said to be isotropic if V contains an isotropic vector. If V contains no isotropic vectors, then the space (V, f) is anisotropic.*

2.2.3 Definition. *A hyperbolic plane, $\mathbb{H}$, over K is a two dimensional $\lambda-$hermitian space which has a basis $\{u, v\}$ with $f(u, u) = f(v, v) = 0$ and $f(u, v) = 1$. The vectors u and v are called a hyperbolic pair.*

The following discussion shows that for an isotropic vector x in a $\lambda-$hermitian space (V, f), a vector y can be found such that $\{x, y\}$ is a hyperbolic pair. First, Lemma 2.2.4 pertains to the specific case when $\lambda = -1$ and $^* = 1$. Such a $\lambda-$hermitian space is called a symplectic space.

2.2.4 Lemma. *Every nonzero vector in a symplectic space is isotropic.*

Proof. Let (V, f) be a symplectic space. By definition of the space, $f(x, x)^* = f(x, x) = -f(x, x)$ for every $0 \neq x \in V$. Hence, $2f(x, x) = 0$. Thus, $f(x, x) = 0$ since K is not of characteristic two. □

Therefore, every symplectic space is clearly isotropic. Also, since the symplectic space (V, f) is assumed to be nonsingular, for any vector x in V there is a $y \in V$ such that $f(x, y) = 1$. In light of Lemma 2.2.4, $\{x, y\}$ is a hyperbolic pair. Further, this result is expanded to nonsymplectic $\lambda-$hermitian spaces in the following proposition.

2.2.5 Proposition. *Let (V, f) be a $\lambda-$hermitian space. If x is an isotropic vector in V, then there exists $y \in V$ such that $\{x, y\}$ is a hyperbolic pair.*

Proof. The previous discussion provides the result for symplectic spaces, so let (V, f) be a nonsymplectic $\lambda-$hermitian space. Since (V, f) is nonsingular, there exists a vector $z \in V$ so that $f(x, z) = 1$. If z is isotropic, then taking $y = z$ achieves the desired result. So suppose z is anisotropic. Let $\gamma = -2^{-1}f(z, z)$ and consider the vector $y = z + \gamma x$. The vector y is equal to 0 if and only if $2z = -f(z, z)x$. But if $2z = -f(z, z)x$, then $2 = f(x, 2z) = f(x, -f(z, z)x) = -f(z, z)^* f(x, x) = 0$. Thus, $y = z + \gamma x \neq 0$ since K has odd characteristic.

Now, $f(y, y) = f(z + \gamma x, z + \gamma x) = f(z, z) + \gamma^* f(z, x) + \gamma f(x, z)$ $+\gamma\gamma^* f(x, x) = f(z, z) + \gamma^*\lambda^* + \gamma = f(z, z) - f(z, z) = 0$. Also, $f(x, y) = f(x, z + \gamma x) = f(x, z) + \gamma^* f(x, x) = 1$. Therefore,$\{x, y\}$ is a hyperbolic pair. □

It follows directly from Proposition 2.2.5 that when (V, f) is a nonsymplectic $\lambda-$hermitian space and $dimV = 2, V$ is isotropic if and only if $V = \mathbb{H}$.

3. Classification and the Special $\lambda-$Hermitian Spaces.

2.3.1 Definition. *Two $\lambda-$hermitian spaces (V, f_1) and (W, f_2) are said to be* <u>isometric</u>*, denoted $V \cong W$, if there is an isomorphism $\varphi : V \longrightarrow W$ such that*

$f_2(\varphi(x), \varphi(y)) = f_1(x, y)$ for every $x, y \in V$. The isomorphism φ is called an <u>isometry.</u>

The isometric relationship $\cong$ clearly defines an equivalence relation on the collection of $\lambda-$hermitian spaces over K. The question then becomes how to classify $\lambda-$hermitian spaces up to isometry. The answer to this question is not completely known for general fields. So at this point, K must again be assumed to be finite, in which case the classification is completely known.

Moreover, attention is now focused on the special $\lambda-$hermitian spaces needed for the study of unitary groups. They are the quadratic, symplectic, and hermitian spaces. Recall that a symplectic space was previously defined as a $-1-$hermitian space with $* = 1$. A quadratic space is a $1-$hermitian space with $* = 1$. Finally, the term hermitian space will be used to describe a $1-$hermitian space over K with $* \neq 1$.

Now in the case of quadratic spaces, it is well known that two spaces are isometric if and only if their dimensions and discriminants are equal [17].

2.3.2 Definition. *Let (V, f) be a quadratic space and $\mathcal{B}$ a basis of V. The <u>discriminant</u> of V is $d\dot{K}^2$ in $\dot{K}/\dot{K}^2$ where $d = detM_{\mathcal{B}}$.*

Considering Proposition 2.1.11, this definition makes sense. There one sees that for any two bases $\mathcal{B}$ and $\mathcal{B}'$ of $V, detM_{\mathcal{B}'} = det(P^tM_{\mathcal{B}}P^*) = (detP)^2detM_{\mathcal{B}}$. This is true since $detP^t = detP$ and $P^* = P$ since $* = 1$. Thus, the discriminant for any two bases differ only by the square of a nonzero element of K. Therefore, as an element of $\dot{K}/\dot{K}^2$, is independent of the choice of basis. Because of the uniqueness of the discriminant dV for a quadratic space (V, f), it has been shown that there are only two distinct types of spaces for any given dimension n up to isometry. It is the case that $V \cong \langle 1, 1, \ldots, 1\rangle$ (n ones) or $V \cong \langle 1, 1, \ldots, 1, \delta\rangle$ ($n-1$

ones) where $\delta \in \dot{K}\backslash\dot{K}^2$[11]. Here the notation $\langle a_1, \cdots, a_n\rangle$ means that there exists an orthogonal basis $\{v_1, \cdots v_n\}$ of V such that $f(v_i, v_i) = a_i$ for $i = 1, \ldots, n$.

In the case of hermitian spaces over K, one simply needs dimension in order to classify spaces. As is shown in the following proposition, this is due to the fact that an orthogonal basis, known to exist by Proposition 2.1.7, can be converted into an orthonormal basis.

2.3.3 Proposition. *Let (V, f) be an n dimensional hermitian space over K. Then V has an orthonormal basis.*

Proof. Let $\{v_1, v_2, \cdots, v_n\}$ be an orthogonal basis of V. $f(x,x)^* = f(x,x)\,\forall\, x \in V$ since V is hermitian. So, for $i = 1, \cdots, n$, $f(v_i, v_i) = a_i \in K_0$. By the surjectivity of the norm map shown in Lemma 1.1.3, there exists an $\alpha_i \in K$ such that $N(\alpha_i) = a_i$. Hence, $\{v_1', v_2', \cdots, v_n'\}$ is an orthonormal basis for V where $v_i' = \dfrac{1}{\alpha_i}v_i$ since$f(v_i', v_i') = f\left(\dfrac{1}{\alpha_i}v_i, \dfrac{1}{\alpha_i}v_i\right) = \dfrac{1}{\alpha_i\alpha_i^*}f(v_i, v_i) = \dfrac{1}{N(\alpha_i)}a_i = \dfrac{1}{a_i}a_i = 1.$ □

Thus, there is only one distinct hermitian space up to isometry for any given dimension n. Namely, for $dimV = n$, $V \cong \langle 1, 1, \cdots, 1\rangle$ (n ones).

The following proposition provides a similar, but more general result for $\lambda-$hermitian spaces over k where $* \neq 1$.

2.3.4 Proposition. *Let (V, f) be an n dimensional $\lambda-$hermitian space over K where $* \neq 1$. Then there exists an $a \in \dot{K}$ such that $V \cong \langle a, a, \ldots, a\rangle (n$ a's).*

Proof. Again let $\{v_1, v_2, \cdots, v_n\}$ be an orthogonal basis of V. By Hilbert's Theorem 90, there exists a $k \in \dot{K}$ such that $k(k^*)^{-1} = \lambda$ since $\lambda\lambda^* = N(\lambda) = 1$. Thus, let $a = k^*$. Then $\Gamma(a) = a^*a^{-1} = (k^*)^*(k^*)^{-1} = k(k^*)^{-1} = \lambda$. $f(v_i, v_i) = b_i \neq 0$ for $i = 1, \ldots, n$ since $* \neq 1$ and V is nonsingular. Further, $\Gamma(b_i) = b_i^*b_i^{-1} = f(v_i, v_i)^*f(v_i, v_i)^{-1} = \lambda$ for $i = 1, \ldots, n$ by definition of the $\lambda-$hermitian form

f. Hence, $a^{-1}b_i \in ker(\Gamma) = \dot{K}_0 = N(\dot{K})$ for $i = 1$ to $i = n$, because the norm map is surjective. This implies that for $1 \leq i \leq n$, there exists $c_i \in \dot{K}$ such that $N(c_i) = a^{-1}b_i$. Thus, $b_i = aN(c_i)$ for $i = 1, \ldots, n$. Therefore, $\{v_1', \ldots, v_n'\}$ where $v_i' = c_i^{-1}v_i$ is the desired orthogonal basis, since $f(v_i', v_i') = f(c_i^{-1}v_i, c_i^{-1}v_i) = (N(c_i))^{-1}f(v_i, v_i) = (N(c_i))^{-1}b_i = a$. Whence, $V \cong \langle a, \ldots, a \rangle$ (n a's). □

It is important to note here also that, in this context, any two dimensional $\lambda-$hermitian space where $^* \neq 1$ is isotropic. This is due to the fact that $-1 \in K_0$ and, hence, there exists $\gamma \in \dot{K}$ such that $N(\gamma) = -1$. Since the space is isometric to $\langle a, a \rangle$ for some $a \in \dot{K}$, there exists an orthogonal basis $\{v_1, v_2\}$ where $f(v_1, v_1) = f(v_2, v_2) = a$. Therefore, $f(v_1+\gamma v_2, v_1+\gamma v_2) = f(v_1, v_1)+\gamma^* f(v_1, v_2)+\gamma f(v_2, v_1) + \gamma\gamma^* f(v_2, v_2) = a - a = 0$. As before, $v_1 + \gamma v_2 \neq 0$ since $v_1 + \gamma v_2 = 0$ would imply $a = f(v_1, v_1) = f(-\gamma v_2, -\gamma v_2) = \gamma\gamma^* f(v_2, v_2) = -a$ and K is not of characteristic two.

Finally, consider the classification of symplectic spaces over K. Here, as in the case of hermitian spaces, only dimension is needed in order to classify spaces.

2.3.5 Proposition. *Every symplectic space is the orthogonal sum of hyperbolic planes and, therefore, even dimensional and up to isometry determined by its dimension.*

Proof. It follows from Lemma 2.2.4 and its subsequent discussion that one can construct a basis of hyperbolic pairs. This is known as a symplectic basis. This fact and the orthogonal decomposition provided by Proposition 2.1.9 shows that every symplectic space is the orthogonal direct sum of hyperbolic planes and, therefore, even dimensional. Further, it is well known that any two hyperbolic planes are isometric [15]. Thus, up to isometry, there is only one distinct space of a given even dimension. □

Chapter 3

The Unitary Group and its Generators

Chapter 1 established some key facts about the underlying finite field K, while Chapter 2 highlighted properties of the λ-hermitian spaces (V, f) over K. Chapter 3 will now introduce the concept of the unitary group.

The chapter has two subsections. The first formalizes the notion of the unitary group of a $\lambda-$hermitian space, while the second defines some of the generating maps of the unitary group. Finally, the subsection concludes with some useful identities involving these generating maps.

1. The Unitary Group.

Let K be a finite field of odd characteristic with involution $*$. View K as a quadratic extension of its fixed field K_0. Let V be an n dimensional nonsingular $\lambda-$hermitian space over K with $\lambda-$hermitian form f. Recall from the previous chapter that an isomorphism φ from a λ-hermitian space V to a $\lambda-$hermitian space W which preserves the "distance" between vectors is called an isometry. The set of isometries from a space V onto itself form a group with respect to composition.

3.1.1 Definition. *Let (V, f) be a $\lambda-$hermitian space. The collection of isometries from V onto itself is called the unitary group of V, denoted $U(V)$.*

If V is a quadratic space (i.e. $\lambda = 1,^* = 1$), then the unitary group $U(V)$ is called the orthogonal group $O(V)$. If V is a symplectic space (i.e. $\lambda = -1$, $* = 1$), then $U(V)$ is called the symplectic group $Sp(V)$. Sometimes $U(V)$ will be referred to as $U_n(V)$ when information about dimension is pertinent. At other times $U(V)$ will be referred to as $U_f(V)$ when information about the λ-hermitian form f is important.

Now when the involution $*$ on K is the identity, λ must equal $+1$ or -1. This is because $f(x,y)^* = f(x,y) = \lambda f(y,x) = \lambda\lambda f(x,y)$. Thus, $f(x,y) = \lambda^2 f(x,y)$ for every $x,y \in V$. Hence, $\lambda = \pm 1$. This, of course, gives rise to a quadratic space with its orthogonal group in the case $\lambda = 1$ and a symplectic space with its symplectic group when $\lambda = -1$.

Consider, then, when the involution on K is different from the identity. In this case, in fact, one can assume that $\lambda = 1$. For when $*$ is not the identity, recall that Hilbert's Theorem 90 guarantees the existence of $k \in K$ such that $k(k^*)^{-1} = \lambda$ since $\lambda\lambda^* = N(\lambda) = 1$. Thus, one can replace the λ−hermitian f with the proportional form $g = kf$. For $x, y \in V$, one sees that $g(x,y)^* = (kf(x,y))^* = k^* f(x,y)^* = k^*\lambda f(y,x) = kf(y,x) = g(y,x)$. Thus, g is a 1-hermitian form.

Further, the following proposition shows that scaling the λ−hermitian form in this way does not affect the unitary group.

3.1.2 Proposition. *Let (V,f) be a λ−hermitian space and $k \in \dot{K}$. Then $U_f(V) = U_{kf}(V)$.*

Proof. Let $\sigma \in U_f(V)$. That means $f(\sigma(x), \sigma(y)) = f(x,y)\ \forall\ x,y \in V$. Thus, $kf(\sigma(x), \sigma y)) = kf(x,y)$. Hence, $\sigma \in U_{kf}(V)$ and $U_f(V) \subseteq U_{kf}(V)$.

Now consider $\sigma \in U_{kf}(V)$. If $\sigma \in U_{kf}(V)$, then $kf(\sigma(x), \sigma(y)) = kf(x,y)\ \forall\ x,y \in V$. However, multiplying both sides of the equation by the field element k^{-1} gives $f(\sigma(x), \sigma(y)) = f(x,y)\ \forall\ x,y \in V$. Thus, $\sigma \in U_f(V)$ and $U_{kf}(V) \subseteq U_f(V)$. Therefore, $U_f(V) = U_{kf}(V)$. □

2. Generators of the Unitary Group.

Let $U_n(V)$ be the unitary group of an n−dimensional λ−hermitian space (V,f) over a finite field K with involution $* \neq 1$. From Chapter 2, one observes that if $n \geq 2$ then the hyperbolic rank of V is at least one. Hence, V splits as

$V = \mathbb{H} \perp L$, where $\mathbb{H}$ is a hyperbolic plane with a hyperbolic pair $\{u, v\}$, namely, $\mathbb{H} = Ku \oplus Kv$ with $f(u,u) = f(v,v) = 0$ and $f(u,v) = 1$.

With this structure in mind, the isometries to be used in the study of $U(V)$ are now defined. Let $\triangle$ denote the isometry such that $\triangle(u) = v, \triangle(v) = \lambda^* u$ and $\triangle|_L = 1$. For nonzero ϵ in K define $\phi[\epsilon]$ in $U(V)$ by $\phi[\epsilon](u) = \epsilon u, \phi[\epsilon](v) = (\epsilon^*)^{-1} v$ and $\phi[\epsilon]|_L = 1$. Recall $C = \{c \in K \mid c + \lambda c^* = 0\}$ from Chapter 1 and for c in C define a transvection $T[u,c]$ in $U(V)$ by

$$T[u,c](z) = z + f(z,u)cu \text{ for } z \in V.$$

For x in L the Eichler transformation $E[u,x]$ in $U(V)$ is defined by

$$E[u,x](z) = z - \lambda\ f(z,u)x + f(z,x)u - \lambda f(z,u)q(x)u$$

for $z \in V$, where $q(x) = 2^{-1}f(x,x)$. Similarly, define $T[v,c] = \triangle T[u,c]\triangle^{-1}$ and $E[v,x] = \triangle E[u,x]\triangle^{-1}$. Finally, for a vector x in V with $q(x) \neq 0$, define the symmetry $\tau[x]$ by the formula

$$\tau[x](z) = z - f(z,x)q(x)^{-1}x \text{ for } z \text{ in } V.$$

The remainder of the chapter is devoted to establishing some identities involving the above isometries which will prove useful in Chapter 4.

3.2.1 Lemma. $T[u,c]T[u,d] = T[u,c+d]$.

Proof. For any $z \in V$,

$$\begin{aligned} T[u,c](T[u,d](z)) &= z + f(z,u)du + f(z + f(z,u)du, u)cu \\ &= z + f(z,u)du + f(z,u)cu + f(u,u)f(z,u)d^*cu \\ &= z + f(z,u)du + f(z,u)cu \quad (\text{since } f(u,u) = 0) \\ &= z + f(z,u)(c+d)u \\ &= T[u,c+d](z). \quad \square \end{aligned}$$

3.2.2 Lemma. *$\sigma T[u,c]\sigma^{-1} = T[\sigma(u),c]$, for any $\sigma \in U(V)$.*

Proof. For any $z \in V$,

$$\begin{aligned}(\sigma T[u,c]\sigma^{-1})(z) &= \sigma(\sigma^{-1}(z) + f(\sigma^{-1}(z),u)cu) \\ &= z + f(z,\sigma(u))c\sigma(u) \\ &= T[\sigma(u),c](z). \quad \square\end{aligned}$$

3.2.3 Lemma. *$T[au,c] = T[u,a^*ca]$, for any $a \in K$.*

Proof. For any $z \in V$,

$$\begin{aligned}T[au,c](z) &= z + f(z,au)cau \\ &= z + f(z,u)a^*cau \\ &= T[u,a^*ca](z). \quad \square\end{aligned}$$

Note here that there are corresponding lemmas to 3.2.2 and 3.2.3 involving $T[v,c]$. Their verifications proceed exactly the same way by replacing u with v. These corresponding lemmas will be referred to as 3.2.2′ and 3.2.3′ respectively.

3.2.4 Lemma. $\phi[\epsilon]T[u,c]\phi[\epsilon]^{-1} = T[\epsilon u,c]$.

Proof.

$$\begin{aligned}\phi[\epsilon]T[u,c]\phi[\epsilon]^{-1} &= T[\phi[\epsilon](u),c] \text{ by Lemma 3.2.2} \\ &= T[\epsilon u,c]. \quad \square\end{aligned}$$

3.2.5 Lemma. $\phi[\epsilon]T[v,c]\phi[\epsilon]^{-1} = T[(\epsilon^*)^{-1}v, c]$.

Proof.

$$\begin{aligned}\phi[\epsilon]T[v,c]\phi[\epsilon]^{-1} &= T[\phi[\epsilon](v), c] \text{ by Lemma 3.2.2}'\\ &= T[(\epsilon^*)^{-1}v, c]. \quad \square\end{aligned}$$

3.2.6 Lemma. $\phi[\epsilon]\triangle\phi[\epsilon]^{-1} = \phi[\epsilon^*\epsilon]\triangle$.

Proof. Since all the maps here restrict to 1_L on L, it suffices to show that the maps agree on the basis vectors u and v of $\mathbb{H}$.

$$\begin{aligned}\phi[\epsilon]\triangle\phi[\epsilon]^{-1} &: u \longrightarrow \epsilon^{-1}u \longrightarrow \epsilon^{-1}v \longrightarrow \epsilon^{-1}((\epsilon^*)^{-1}v) = (\epsilon^*\epsilon)^{-1}v\\ &: v \longrightarrow (\epsilon^*)v \longrightarrow (\epsilon^*)(\lambda^*u) \longrightarrow \epsilon^*\lambda^*\epsilon u = \lambda^*\epsilon^*\epsilon u.\end{aligned}$$

$$\begin{aligned}\phi[\epsilon^*\epsilon]\triangle &: u \longrightarrow v \longrightarrow ((\epsilon^*\epsilon)^*)^{-1}v = (\epsilon^*\epsilon)^{-1}v\\ &: v \longrightarrow \lambda^*u \longrightarrow \lambda^*\epsilon^*\epsilon u. \quad \square\end{aligned}$$

3.2.7 Lemma. $\phi[a]\phi[b] = \phi[b]\phi[a]$.

Proof. Here again all maps restrict to 1_L on L; thus, agreement on u and v need only be shown.

$$\begin{aligned}\phi[a]\phi[b] &: u \longrightarrow bu \longrightarrow bau = abu\\ &: v \longrightarrow (b^*)^{-1}v \longrightarrow (b^*)^{-1}(a^*)^{-1}v = ((ab)^*)^{-1}v\end{aligned}$$

$$\begin{aligned}\phi[b]\phi[a] &: u \longrightarrow au \longrightarrow abu\\ &: v \longrightarrow (a^*)^{-1}v \longrightarrow (a^*)^{-1}(b^*)^{-1}v = ((ab)^*)^{-1}v. \quad \square\end{aligned}$$

3.2.8 Lemma. $E[u, x+y] = E[u,x]E[u,y]$ if $f(x,y) = f(y,x)$.

Proof. For any $z \in V$,

$$\begin{aligned} E[u,x](E[u,y](z)) =& E[u,y](z) - \lambda f(E[u,y](z),u)x \\ & + f(E[u,y](z),x)u - \lambda f(E[u,y](z),u)q(x)u \end{aligned}$$

$$\begin{aligned} &= z - \lambda f(z,u)y + f(z,y)u - \lambda f(z,u)q(y)u \\ &- \lambda f(z - \lambda f(z,u)y + f(z,y)u - \lambda f(z,u)q(y)u, u)x \\ &+ f(z - \lambda f(z,u)y + f(z,y)u - \lambda f(z,u)q(y)u, x)u \\ &- \lambda f(z - \lambda f(z,u)y + f(z,y)u - \lambda f(z,u)q(y)u, u)q(x)u \end{aligned}$$

$$\begin{aligned} &= z - \lambda f(z,u)y + f(z,y)u \qquad -\lambda f(z,u)q(y)u \\ &\quad -\lambda f(z,u)x \\ &\qquad\qquad + f(z,x)u \qquad\qquad\qquad \lambda f(z,u)f(y,x)u \\ &\qquad\qquad\qquad\qquad -\lambda f(z,u)q(x)u \end{aligned}$$

(since $f(u,u) = f(u,x) = f(x,u) = f(u,y) = f(y,u) = 0$)

$$= z - \lambda f(z,u)(x+y) + f(z,x+y)u - \lambda f(z,u)q(x+y)u$$

(since $f(y,x) = f(x,y)$)

$$= E[u,x+y](z). \quad \square$$

3.2.9 Lemma. *$\sigma E[u,x]\sigma^{-1} = E[\sigma(u), \sigma(x)]$, for any $\sigma \in U(V)$.*

Proof. For any $z \in V$,

$$\begin{aligned}\sigma E[u,x]\sigma^{-1}(z) &= \sigma(\sigma^{-1}(z) - \lambda f(\sigma^{-1}(z), u)x + f(\sigma^{-1}(z), x)u \\ &\qquad - \lambda f(\sigma^{-1}(z), u)q(x)u \\ &= z - \lambda f(z, \sigma(u))\sigma(x) + f(z, \sigma(x))\sigma(u) \\ &\qquad - \lambda f(z, \sigma(u))q(x)\sigma(u) \\ &= E[\sigma(u), \sigma(x)](z). \quad \square\end{aligned}$$

3.2.10 Lemma. *$E[au, x] = E[u, a^*x]$, for any $a \in K$.*

Proof. For any $z \in V$,

$$\begin{aligned}E[au,x](z) &= z - \lambda f(z, au)x + f(z,x)au - \lambda f(z, au)q(x)au \\ &= z - \lambda f(z,u)a^*x + f(z, a^*x)u - \lambda f(z,u)a^*aq(x)u \\ &= z - \lambda f(z,u)a^*x + f(z, a^*x)u - \lambda f(z,u)q(a^*x)u \\ &= E[u, a^*x](z). \quad \square\end{aligned}$$

Again, there are corresponding lemmas involving $E[v,x]$ which are found by replacing u by v in Lemmas 3.2.9 and 3.2.10. These will be referred to as 3.2.9′ and 3.2.10′.

3.2.11 Lemma. *$\phi[\epsilon]E[u,x]\phi[\epsilon]^{-1} = E[u, \epsilon^* x]$.*

Proof.

$$\begin{aligned}\phi[\epsilon]E[u,x]\phi[\epsilon]^{-1} &= E[\phi[\epsilon](u), \phi[\epsilon](x)] \text{ by Lemma 3.2.9} \\ &= E[\epsilon u, x] \text{ since } x \in L \\ &= E[u, \epsilon^* x] \text{ by Lemma 3.2.10.} \quad \square\end{aligned}$$

3.2.12 Lemma. $\phi[\epsilon]E[v,x]\phi[\epsilon]^{-1} = E[v,\epsilon^{-1}x]$.

Proof.

$$\begin{aligned} \phi[\epsilon]E[v,x]\phi[\epsilon]^{-1} &= E[\phi[\epsilon](v),\phi[\epsilon](x)] \text{ by Lemma 3.2.9}' \\ &= E[(\epsilon^*)^{-1}v,x] \text{ since } x \in L \\ &= E[v,\epsilon^{-1}x] \text{ by Lemma 3.2.10}'. \quad \square \end{aligned}$$

CHAPTER 4

TWO-ELEMENT GENERATION OF $U(V)$

Now that all of the necessary frame work for the underlying finite field, the $\lambda-$hermitian space over this field and the space's unitary group has been established, Chapter 4 provides a detailed discussion of the paper's main result. The chapter two subsections separate some preliminary information and statement of the main theorem from the theorem's proof.

1. Preliminaries.

Let K be a finite field of odd characteristic with involution $*$. Thus $|K| = q = p^m$ for some odd prime p and natural number m. Recall from Chapter 1 that K is a quadratic extension field of K_0, the fixed field of $*$. In this context, when $* \neq 1$, $*$ is the Fröbenius automorphism σ defined by $\sigma(a) = a^\ell$ for $a \in K$ where $|K_0| = \ell$. Let α, β be fixed generators of the multiplicative cyclic groups $\dot{K}$ and $\dot{K}_0$ respectively. Moreover, let (V, f) be an $n-$dimensional, nonsingular $\lambda-$hermitian space over K with its unitary group $U_n(V)$.

Further, it is assumed that $n \geq 2$. This is due to the fact that $U_1(V)$ is cyclic and, thus, has a single generating element. To see this, consider that for an isometry φ in $U_1(V), \varphi$ must be defined for $z \in V$ by $\varphi(z) = az$ where $a \in \dot{K}$ such that $N(a) = aa^* = 1$. In this case, $f(\varphi(x), \varphi(y)) = f(ax, ay) = aa^* f(x, y) = f(x, y.)$ for all $x, y \in V$. Thus, there is a canonical isomorphism between the isometries of $U_1(V)$ and the elements of norm 1 in $\dot{K}$. Let G be the subset of $\dot{K}$ containing elements of norm 1. For $a, b \in G$, $(ab^{-1})^* ab^{-1} = a^*(b^{-1})^* ab^{-1} = a^* a (b^{-1})^* b^{-1} = (b^* b)^{-1} = 1^{-1} = 1$. Hence, G is a multiplicative subgroup of the multiplicative, cyclic group $\dot{K}$ and is, therefore, cyclic. This, of course, means $U_1(V)$ is cyclic as well.

The problem of two-generating unitary groups for $n \geq 2$ has been shown in part by the works of Ishibashi [12], Earnest and Ishibashi [7], and Earnest et. al. [2]. In [12], Ishibashi proved that if (V, f) is a nonsingular, isotropic, λ-hermitian space over a finite field of odd characteristic with involution *, then the unitary group $U(V)$ is generated by three elements. Further, in fact, he proved that when the unitary group is the symplectic group $Sp(V)$ then $U(V)$ is generated by just two elements. His result is worded below for further reference.

4.1.1 Theorem. (Ishibashi) *$U(V)$ is generated by 3 elements and $U(V) = Sp(V)$ is generated by 2 elements.*

In [7] and [2], the case where the unitary group is the orthogonal group was considered. Here, the restrictions of isotropy and characteristic were removed. The following refinement of theorem 4.1.1 was achieved.

4.1.2 Theorem. (Earnest/Ishibashi et.al) $U(V) = O(V)$ is generated by two elements.

In this chapter, it is Theorem 4.1.1 which is again further refined with the following result.

4.1.3 Theorem. *$U(V)$ is generated by two elements.*

Although the unitary groups of Theorem 4.1.3 are still restricted to $\lambda-$hermitian spaces over finite fields of characteristic not two, the $\lambda-$hermitian spaces no longer need the explicit assumption of isotropy. Recall from Chapter 3 that unitary groups of symplectic, quadratic and $\lambda-$hermitian spaces where $* \neq 1$ are all that is necessary to consider. Isotropy for all symplectic spaces was shown in Chapter 2. Also, the two-generation problem of orthogonal groups for isotropic as well as anisotropic quadratic spaces was solved by Theorem 4.2.2. Finally, for $n = 2$, a λ–hermitian space where $* \neq 1$ is isometric to the hyperbolic plane by the discussions subsequent to Propositions 2.3.4 and 2.2.4 respectively. Thus for dimensions greater than 2, a λ–hermitian space where $* \neq 1$ splits as $\mathbb{H} \perp L$.

Further, Proposition 2.3.4 allows for the assumption that L has an orthogonal basis such that $L \cong \langle a, a, \ldots, a\rangle(n-2$ a's for some $a \in \dot{K}$ If $X = \{x_1, x_2, \ldots, x_{n-2}\}$ is such a base for L, then one can define an isometry in $U(L)$ which permutes these basis vectors since $f(x_i, x_i) = f(x_j, x_j) = a$ for any choice of i and j. These kinds of isometries will prove to be particularly useful in generating the unitary group of a hermitian space.

2. Proof of the Main Theorem.

The proof of Theorem 4.1.3 breaks down into three parts. The first part is when $* = 1$ and $\lambda = -1$ (i.e. $U(V) = Sp(V)$). This part is proven by Theorem 4.1.1. Part 2 is when $* = 1$ and $\lambda = 1$. (i.e. $U(V) = O(V)$). Part 2 is proven by Theorem 4.1.2. The third part boils down to $* \neq 1$. That is, when $U(V) \neq Sp(V)$ and $U(V) \neq O(V)$.

It is part 3 to which the remainder of this chapter is devoted to achieving. The proof of part 3 breaks down into three cases based on the dimension n of V over K. They are $n = 2$, $n > 2$ even, and $n \geq 3$ odd. The odd dimensional case will be treated first because of its relative simplicity.

4.2.1 Lemma. *Let $x \in L$ and $\sigma \in U(L)$. Then the subgroup generated by $\phi[\alpha]$ and $\triangle E[u, x]\sigma$ contains $\triangle\sigma$ and $E[v, Kx]$.*

Proof. Let $G = \langle \phi[\alpha],\ \triangle E[u, x]\sigma\rangle$.

First, the following conjugation will be shown by induction:

$$\phi[\alpha]^i \Delta E[u,x]\sigma\phi[\alpha]^{-i} = \phi[\alpha^*\alpha]^i \Delta E[u,(\alpha^*)^i x]\sigma. \qquad (1)$$

Let $i = 1$. $\phi[\alpha]\Delta E[u,x]\sigma\phi[\alpha]^{-1}$

$$=\phi[\alpha]\Delta\phi[\alpha]^{-1}\phi[\alpha]E[u,x]\phi[\alpha]^{-1}\phi[\alpha]\sigma\phi[\alpha]^{-1}$$

$=\phi[\alpha^*\alpha]\Delta E[u,\alpha^* x]\sigma$ by Lemmas 3.2.6 and 3.2.11.

Now suppose $\phi[\alpha]^{i-1}\Delta E[u,x]\sigma\phi[\alpha]^{-i+1} = \phi[\alpha^*\alpha]^{i-1}\Delta E[u,(\alpha^*)^{i-1}x]\sigma$. Consider $\phi[\alpha]^i\Delta E[u,x]\sigma\phi[\alpha]^{-i}$.

$\phi[\alpha]^i\Delta E[u,x]\sigma\phi[\alpha]^{-i} = \phi[\alpha]\phi[\alpha]^{i-1}\Delta E[u,x]\sigma\phi[\alpha]^{-i+1}\phi[\alpha]^{-1}$

$= \phi[\alpha]\phi[\alpha^*\alpha]^{i-1}\Delta E[u,(\alpha^*)^{i-1}x]\sigma\phi[\alpha]^{-1}$ (by the inductive hypothesis)

$= \phi[\alpha^*\alpha]^{i-1}\phi[\alpha]\Delta E[u,(\alpha^*)^{i-1}x]\sigma\phi[\alpha]^{-1}$ (by Lemma 3.2.7)

$= \phi[\alpha^*\alpha]^i\Delta E[u,(\alpha^*)^i x]\sigma$ as in the case $i = 1$.

Thus, equation (1) is true for every $i \geq 1$. But, $\phi[\alpha^*\alpha] = \phi[\alpha^\ell\alpha] = \phi[\alpha^{\ell+1}]$ $\phi[\alpha]^{\ell+1}$. Hence, for every $i \geq 1, \phi[\alpha]^i\Delta E[u,x]\sigma\phi[\alpha]^{-i} = \phi[\alpha]^{(\ell+1)i}\Delta E[u,\alpha^{\ell i}x]\sigma$. However, this implies $\Delta E[u,\alpha^{\ell i}x]\sigma \in G$ for every $i \geq 1$. Therefore, $\Delta E[u,\dot{K}x]\sigma \subseteq G$.

So, for $\gamma \in \dot{K}$, $(\Delta E[u,2\gamma x]\sigma)(\Delta E[u,\gamma x]\sigma)^{-1} \in G$, since the characteristic of K is not 2. But $(\Delta E[u,2\gamma x]\sigma)(\Delta E[u,\gamma x]\sigma)^{-1}$

$= \Delta E[u,2\gamma x]\sigma\sigma^{-1}E[u,-\gamma x]\Delta^{-1} = \Delta E[u,2\gamma x]E[u,-\gamma x]\Delta^{-1}$

$= \Delta E[u,\gamma x]\Delta^{-1}$ (by Lemma 3.2.8 since $f(2\gamma x,-\gamma x) = -2\gamma\gamma^* f(x,x)$

$= f(-\gamma x, 2\gamma x))$

$= E[v,\gamma x]$ by Lemma 3.2.9. Whence, $E[v,\dot{K}x] \subseteq G$.

Moreover,$E[v,0x] = 1 \in G$. Thus $E[v,Kx] \subseteq G$.

Finally, $E[v,-x]\Delta E[u,x]\sigma \in G$. However, $E[v,-x]\Delta E[u,x]\sigma =$ $E[v,-x]\Delta E[u,x]\Delta^{-1}\Delta\sigma = E[v,-x]E[v,x]\Delta\sigma = \Delta\sigma$. □

4.2.2 Proposition. *Let $n \geq 3$ be odd. Then $U_n(V)$ is generated by $\phi[\alpha]$ and $\Delta E[u,x_1]\sigma$ where $\sigma: x_1 \to x_2 \to \cdots \to x_{n-2} \to x_1$ for some orthogonal basis of L with $f(x_i,x_i) = f(x_j,x_j), 1 \leq i,j \leq n-2$.*

Proof. Let $G = \langle \phi[\alpha], \Delta E[u,x_1]\sigma\rangle$. By Lemma 4.2.1, $\Delta\sigma$ and $E[v,Kx_1]$ are contained in G. It suffices to show that $E[u,x_1]$ is also contained in G, since it is already known that $U_n(V) = \langle \phi[\alpha], \Delta\sigma, E[u,x_1]\rangle$ by [12; Proposition 3.2] in this case.

Now, $E[v,Kx_1] \subseteq G$ implies that $E[v,\lambda^{-1}x_1] \in G$. Conjugating this element by $\Delta\sigma$, one gets

$$\begin{aligned}\Delta\sigma E[v,\lambda^{-1}x_1](\Delta\sigma)^{-1} = \Delta\sigma E[v,\lambda^{-1}x_1]\sigma^{-1}\Delta^{-1} &= \Delta E[v,\lambda^{-1}x_2]\Delta^{-1}\\ &= E[\lambda^* u,\lambda^{-1}x_2] \text{ by Lemma 3.2.9}\\ &= E[u,\lambda\lambda^{-1}x_2] \text{ by Lemma 3.2.10}\\ &= E[u,x_2] \in G.\end{aligned}$$

Continuing this conjugation process will yield $E[u,Kx_i]$ and $E[v,Kx_i]$ for $i = 1,2,...,n-2$. Thus, G contains $E[u,x_1]$ which completes the proof. □

4.2.3 Lemma. *Let $x,y \in L$ with $f(x,y) = f(y,x) = 0$ and $\sigma \in U(L)$, then the subgroup generated by $\phi[\alpha]\tau[x]$ and $\Delta E[u,y]\sigma$ contains $\Delta\sigma$ and $E[v,Ky]$.*

Proof. Let $G = \langle \phi[\alpha]\tau[x], \Delta E[u,y]\sigma\rangle$. Again, consider the conjugation $(\phi(\alpha)\tau[x])^i\Delta E(u,y)\sigma(\phi(\alpha)\tau[x])^{-i}$ which is contained in G.
$(\phi[\alpha]\tau[x])^i\Delta E[u,y]\sigma(\phi[\alpha]\tau[x])^{-i} = \phi[\alpha]^i\tau[x]^i\Delta E[u,y]\sigma\tau[x]^{-i}\phi[\alpha]^{-i}$,
since $\phi[\alpha] \in U(\mathbb{H})$ and $\tau[x] \in U(L)$ and, thus, $\phi[\alpha]\tau[x] = \tau[x]\phi[\alpha]$. Therefore,

$\tau[x]^i\phi[\alpha]^i\triangle E[u,y]\sigma\phi[\alpha]^{-i}\tau[x]^{-i}$ is obtained by the conjugation. But this is equal to $\tau[x]^i\phi[a]^{(\ell+1)i}\triangle E[u,\alpha^{\ell i}y]\sigma\tau[x]^{-i}$ as previously shown in Lemma 4.2.1.

Thus, if i is even, one has $\phi[\alpha]^{(\ell+1)i}\triangle E(u,ay)\sigma$ where $a\in\dot{K}^2$ since ℓi is even. However, this is $(\phi[\alpha]\tau[x])^{(\ell+1)i}\triangle E[u,ay]\sigma$ since $(\ell+1)i$ is even. This implies that $\triangle E[u,ay]\sigma\in G$. Since this can be done for any even integer, $\triangle E[u,\dot{K}^2y]\sigma\subseteq G$.

Now, if i is odd, then $\tau[x]^i\phi[\alpha]^{(\ell+1)i}\triangle E[u,\alpha^{\ell i}y]\sigma\tau[x]^{-i}=\tau[x]\phi[\alpha]^{(\ell+1)i}\triangle E[u,\alpha^{\ell i}y]\sigma\tau[x]$. Further, since ℓ is odd, $\tau[x]\phi[\alpha]^{(\ell+1)i}\triangle E[u,\alpha^{\ell i}y]\sigma\tau[x]$ $=(\phi[\alpha]\tau[x])^{(\ell+1)i}\tau[x]\triangle E[u,\alpha^{\ell i}y]\sigma\tau[x]$. This implies that $\tau[x]\triangle E[u,by]\sigma\tau[x]$ is contained in G where $b\in\dot{K}\backslash\dot{K}^2$.

Let $\gamma\in\dot{K}^2$. If $\gamma\in\dot{K}^2$, then $2\gamma\in\dot{K}^2$ since K has odd characteristic and $2\in\dot{K}_0\subseteq\dot{K}^2$ (Lemma 1.2.8). So $(\triangle E[u,2\gamma y]\sigma)(\triangle E[u,\gamma y]\sigma)^{-1}=E[v,\gamma y]$ is contained in G as shown in Lemma 4.2.1.

Let $\gamma\in\dot{K}\backslash\dot{K}^2$. If $\gamma\in\dot{K}\backslash\dot{K}^2$, then $2\gamma\in\dot{K}\backslash\dot{K}^2$ as above.
So $(\tau[x]\triangle E[u,2\gamma y]\sigma\tau[x])(\tau[x]\triangle E[u,\gamma y]\sigma\tau[x])^{-1}$

$$=\tau[x]\triangle E[u,\gamma y]\sigma\triangle^{-1}\tau[x]\quad\text{by Lemma 3.2.8}$$

$$=\tau[x]E[v,\gamma y]\tau[x]\text{ by Lemma 3.2.9}$$

$$=E[v,\gamma y]\in G\text{ since }f(x,y)=f(y,x)=0.$$

Therefore, $E[v,Ky]$ is again a subset of G.

Finally, $E[v,-y]\triangle E[u,y]\sigma\in G$ since $1\in\dot{K}^2$ and $E[v,-y]\triangle E(u,y)\sigma=\triangle\sigma$ as in Lemma 4.2.1 which ends the proof. □

4.2.4 Proposition. *Let $n > 2$ be even. Assume that $-\lambda = \alpha^{2k+1}$ for some natural number k or $k = 0$. Then $U_n(V)$ is generated by $\phi[\alpha]\tau[x_1 - x_{n-2}]$ and $\Delta E[u, x_2]\sigma$ where $\sigma : x_1 \longrightarrow x_2 \cdots \longrightarrow x_{n-2} \longrightarrow x_1$.*

Proof. Let $G = \langle \phi[\alpha]\tau[x_1 - x_{n-2}], \ \Delta E[u, x_2]\sigma \rangle$. By Lemma 4.2.3, G contains $\Delta\sigma$ and $E[v, Kx_2]$. It only remains to show that G contains $E[u, x_1]$, since $U_n(V) = \langle \phi[\alpha]\tau[x_1 - x_{n-2}], \ \Delta\sigma, \ E[u, x_1] \rangle$ as proven in [12; Proposition 3.3].

Employing the strategy of conjugation by $\Delta\sigma$, one sees $(\Delta\sigma)E[v, Kx_2](\Delta\sigma)^{-1} = \Delta\sigma E[v, Kx_2]\sigma^{-1}\Delta^{-1} = \Delta E[v, Kx_3]\Delta^{-1}$ $= E[\lambda^* u, Kx_3] = E[u, \lambda K x_3]$. Again, the last two equalities come by way of Lemmas 3.2.9 and 3.2.10 as in Proposition 4.2.2. Moreover, $E[u, \lambda K x_3] = E[u, Kx_3]$ since $\lambda \in K$.

By repeating the conjugation and using the fact that $n-2$ is even since n is even, it follows that G contains $E[v, Kx_i]$ where $i = 2, 4, \cdots, n-2$ and $E[u, Kx_j]$ where $j = 1, 3, ..., n-3$. Thus, $E[u, Kx_1]$ is contained in G. So, $E[u, x_1]$ is an element of G.

Note that Lemma 4.2.3 cannot be applied directly when $n = 4$, for then $n - 2 = 2$ and $f(x_1 - x_2, x_2) \neq 0$. However, it can be seen from the proof of that lemma that $E[v, \gamma x_2] \in G$ for all $\gamma \in K^2$. In particular, $E[v, x_2] \in G$, and so $E[v, x_2]^{-1} = E[v, -x_2] \in G$. Then $E[v, -x_2]\Delta E[u, x_2]\sigma = \Delta E[u, -x_2]E[u, x_2]\sigma = \Delta\sigma \in G$. Finally, $(\Delta\sigma)^{-1}E[v, x_2](\Delta\sigma) = E[u, x_1] \in G$ by Lemma 3.2.9. □

4.2.5 Proposition. *Let $n > 2$ be even. Assume that $-\lambda = \alpha^{2k}$ for some natural number k or $k = 0$. Then $U_n(V)$ is generated by $\phi[\alpha]\tau[x_1 - x_{n-2}]$ and $\Delta E[u, x_2]\sigma$ where $\sigma : x_1 \longrightarrow x_2 \longrightarrow \cdots \longrightarrow x_{n-3} \longrightarrow x_1$.*

Proof. Again, let $G = \langle \phi[\alpha]\tau[x_1 - x_{n-2}], \Delta E[u, x_2]\sigma \rangle$. The proof proceeds exactly the same as that in Proposition 4.2.4. Note here, however, that when conjugating by $\triangle\sigma$, one gets $E[v, Kx_i]$ where $i = 2, 4, ..., n-4$ and $E[u, Kx_j]$ where $j = 3, ..., n-3$ contained in G. When $E[u, Kx_{n-3}]$ is conjugated by $\triangle\sigma$, it follows that $E[v, Kx_1]$ is contained in G. Repeating the conjugation on this second pass puts $E[v, Kx_m]$ where $m = 1, 3, \cdots, n-3$ and $E[u, Kx_r]$ where $r = 2, 4, ..., n-4$ in G. Thus, conjugating $E[v, Kx_{n-3}]$ by $\triangle\sigma$ on this second pass places the desired $E[u, Kx_1]$ in G.

As in the proof of Proposition 4.2.4, the case $n = 4$ needs to be treated separately. Note that in this case $\sigma = 1_L$. As before, it has been shown that $E[v, x_2] \in G$. This implies that $E[v, -x_2] \in G$ and $E[v, -x_2]\triangle E[u, x_2] = \triangle E[u, -x_2]E[u, x_2] = \triangle \in G$. As $\tau[x_1 - x_2] = \tau[x_2 - x_1]$, it follows from Proposition 3.4 of [12] that $U_n(V) = \langle \phi[\alpha]\tau[x_1 - x_2], \triangle, E[u, x_2]\rangle$. So it remains only to show that $E[u, x_2] \in G$. But $E[u, x_2] = \triangle^{-1}E[v, x_2]\triangle \in G$, since $E[v, x_2] \in G$ and $\triangle \in G$. □

Finally, in the two dimensional case, it suffices to only look at the generators of $U(\mathbb{H})$. Recall from the previous two chapters that if $dimV = 2$, $V = \mathbb{H}$. In this case, the following result is obtained.

4.2.6 Proposition. *If $C = \{0\}$, then $U(\mathbb{H}) = \langle \triangle, \phi[\alpha]\rangle$; otherwise $U(\mathbb{H}) = \langle \phi[\alpha], \triangle T[u, c]\rangle$ where c is any nonzero element of C.*

Proof. In [10; Lemma 2.3], Ishibashi showed that if $C = \{0\}$, then $U(\mathbb{H}) = \langle \triangle, \phi[\alpha]\rangle$ and if $C \neq \{0\}$, then $U(\mathbb{H}) = \langle \triangle, \phi[\alpha], T[u, c]\rangle$ where $c \in \dot{C}$. It will be shown that in this latter case $U(\mathbb{H}) = \langle \phi[\alpha], \triangle T[u, c]\rangle$.

So let C contain $c \neq 0$. As shown in Chapter 1, $\dot{C} = \{c\beta^i \mid i = 1, 2, ..., \ell - 1\}$ where β is a fixed generator of K_0. Thus, $T[u, \dot{C}] = \{T[u, \beta^i c]\}$. However, consider the conjugation of $\triangle T[u,c]$ by $\phi[\beta]$.

$$\begin{aligned}\phi[\beta]\triangle T[u,c]\phi[\beta]^{-1} &= \phi[\beta]\triangle\phi[\beta]^{-1}\phi[\beta]T[u,c]\phi[\beta]^{-1}\\ &= \phi[\beta^*\beta]\triangle T[\beta u,c] \text{ by Lemmas 3.2.6 and 3.2.4}\\ &= \phi[\beta^2]\triangle T[u,\beta^2 c] \text{ by Lemma 3.2.3 and since } \beta\in K_0.\end{aligned}$$

Suppose $\phi[\beta]^{i-1}\triangle T[u,c]\phi[\beta]^{-i+1} = \phi[\beta^{2(i-1)}]\triangle T[u,\beta^{2(i-1)}c]$. Consider $\phi[\beta]^i\triangle T[u,c]\phi[\beta]^{-i}$.

$$\begin{aligned}&\phi[\beta]^i\triangle T[u,c]\phi[\beta]^{-i} = \phi[\beta]\phi[\beta]^{i-1}\triangle T[u,c]\phi[\beta]^{-i+1}\phi[\beta]^{-1}\\ &= \phi[\beta]\phi[\beta^{2(i-1)}]\triangle T[u,\beta^{2(i-1)}c]\phi[\beta]^{-1} \text{ (by the inductive supposition)}\\ &= \phi[\beta^{2(i-1)}]\phi[\beta]\triangle T[u,\beta^{2(i-1)}c]\phi[\beta]^{-1} \text{ (by Lemma 3.2.7)}\\ &= \phi[\beta^{2(i-1)}]\phi[\beta^2]\triangle T[u,\beta^2\beta^{2(i-1)}c] \text{ (as above)}\\ &= \phi[\beta^{2i}]\triangle T[u,\beta^{2i}c]\\ &= \phi[\beta]^{2i}\triangle T[u,\beta^{2i}c].\end{aligned}$$

Hence, $\phi[\beta]^i\triangle T[u,c]\phi[\beta]^{-i} = \phi[\beta]^{2i}\triangle T[u,\beta^{2i}c]$ for every integer $i\geq 1$ by induction.

This implies that for any $i\geq 1$, $\triangle T[u,\beta^{2i}c]$ is an element of $\langle\phi[\beta],\triangle T[u,c]\rangle$. Further, let r and s be arbitrary even intgers, then $\langle\phi[\beta],\triangle T[u,c]\rangle$ contains $(\triangle T[u,\beta^s c])^{-1}(\triangle T[u,\beta^r c]) = T(u,-\beta^s c)\triangle^{-1}\triangle T(u,\beta^r c) = T(u,(\beta^r-\beta^s)c)$. Thus, $T(u,\mathcal{E}_{K_0}c)\subseteq\langle\phi[\beta],\triangle T[u,c]\rangle$.

If $\mathcal{E}_{K_0} = K_0$, then $T[u,K_0c] = T(u,C)\subseteq\langle\phi[\beta],\triangle T[u,c]\rangle$ by Lemma 1.2.10. Specifically, $T[u,c]\in\langle\phi[\beta],\triangle T[u,c]\rangle$. This, of course, implies that $\triangle\in\langle\phi(\beta),\triangle T(u,c)\rangle$. Moreover, since β is contained in the multaplicative cyclic group,

$\dot{K}$, generated by α, it follows that $\{\Delta, T[u,c]\} \subseteq \langle \phi[\alpha], \Delta T[u,c]\rangle$. This provides the result.

If $\mathcal{E}_{K_0}\backslash\{\pm 1\}$, then for $|K_0| > 3$, there exists $\delta \in K_0$ such that $\delta \neq \pm 1$. Thus, $T[u, \delta c]$ and $T[u,(1-\delta)c]$ are elements of $T[u, \mathcal{E}_{K_0}c]$. Then $T[u,\delta c]T[u,(1-\delta)c] = T[u,c] \in \langle \phi[\beta], \Delta T[u,c]\rangle$ by Lemma 3.2.1. Hence, the argument proceeds as before and $U(\mathbb{H}) = \langle \phi[\alpha], \Delta T[u,c]\rangle$.

Therefore, consider the case when $|K_0| = 3$. Then $K_0 \cong \{-1,0,1\}$ and for ease of discussion, take $K_0 = \{-1,0,1\}$. Suppose, then, that K is a two dimensional extension of $\{-1,0,1\}$. Here, K is a field with 9 elements. In this case also, $\beta = -1$. Now, $N(\alpha) = \alpha\alpha^* = \pm 1$, since the norm map is surjective. But $N(\alpha) = 1$ implies that $N(x) = 1$ for all $x \in \dot{K}$. Thus, $N(\alpha) = -1 = \beta$.

Consider the following conjugation.

$$\begin{aligned}
\phi[\alpha]\Delta T[u,c]\phi[\alpha]^{-1} &= \phi[\alpha]\Delta\phi[\alpha]^{-1}\phi[\alpha]T[u,c]\phi[\alpha]^{-1}\\
&= \phi[\alpha\alpha^*]\Delta T[u,[\alpha\alpha^*]c]\\
&= \phi(\beta)\Delta T(u,\beta c).
\end{aligned}$$

But this implies that $\Delta T[u,\beta c] = \Delta T[u,-c]$ is contained in $\langle \phi[\alpha], \Delta T[u,c]\rangle$ as before. That means $(\Delta T[u,c])^{-1}(\Delta T[u,-c]) = T[u,-c]\Delta^{-1}\Delta T[u,-c]$ $= T[u,-c]T[u,-c] = T[u,c]$ is an element of $\langle \phi[\alpha], \Delta T[u,c]\rangle$. Again, this puts Δ in $\langle \phi[\alpha], \Delta T[u,c]\rangle$ and $U(\mathbb{H}) = \langle \phi[\alpha], \Delta T[u,c]\rangle$. This completes the proof of Proposition 4.2.6. □

Theorem 4.1.3 is now clear by Theorems 4.1.1 and 4.1.2 and Propositions 4.2.2, 4.2.4, 4.2.5, and 4.2.6.

Bibliography

1. R. Baeza, Quadratic Forms over Semilocal Rings, Lecture Notes in Mathematics 655, Springer-Verlag, Berlin/New York, 1978.

2. R.A. Catalpa, A.G. Earnest, G.T. Stewart and U.S. Schmidt, "Minimal Generating Sets for Orthogonal Groups over Finite Fields", J. Algebra 176 (1995), pp. 585-590.

3. J. Dieudonne, La Geometrie des Groupes Classiques, 2nd Ed., Springer-Verlag, New York, 1963.

4. J. Dieudonne, "On the Structure of Unitary Groups", Trans. of the American Math. Soc., Vol. 72 (1952), pp. 367-385.

5. J. Dieudonne, "On the Structure of Unitary Groups II", Trans. of the American Math. Soc., Vol. 73 (1953), pp. 665-678.

6. J. Dieudonne, "Sur les Groupes Classiques", Scientifiques et Industrielles 1040 (1973), pp. 1-84.

7. A.G. Earnest and H. Ishibashi, "Two-Element Generation of Orthogonal Groups over Finite Fields," J. Algebra 165 (1994), pp. 164-171.

8. E.W. Ellers, "Decomposition of Orthogonal, Symplectic, and Unitary Isometries into Simple Isometries", Abh. Math. Sem. Univ. Hamburg 46(1977), pp. 97-127.

9. A.J. Hahn and O.T. O'Meara, The Classical Groups and K. Theory, Grund. Math Wissenschaften 291, Springer-Verlag, Berlin/New York/Tokyo, 1989.

10. H. Ishibashi, "Generation of the Classical Groups over Finite Fields", Linear Algebra Appl. 51(1983), pp. 9-15.

11. H. Ishibashi, "Generators of an Orthogonal Group over a Finite Field", Czech. Math. J. 28(1978), pp. 419-433.

12. H. Ishibashi, "Small Systems of Generators of Isotropic Unitary Groups over Finite Field of Characteristic not Two", J. Algebra 93 (1985), pp. 324-331.

13. H. Ishibashi, "Unitary Groups with Excellent S and Entire E(u,L), J. Algebra 76(1982), pp. 442-458.

14. D.G. James, "Unitary Groups over Local Rings", J. Algebra 52(1978), pp. 354-363.

15. M.A. Knus, Quadratic and Hermitian Forms over Rings, Grund. Math. Wissenschaften 294, Springer-Verlag, Berlin/New York/Tokyo, 1991.

16. L.J. Rylands and D.E. Taylor, "Matrix Generators for the Orthogonal Group", J. Symbolic Computation 25 (1998), pp. 351-360.

17. W. Scharlau, Quadratic and Hermitian Forms, Grund. Math.
Wissenschaften 270, Springer-Verlag, Berlin/Heidelberg/New York/
Tokoyo, 1985.

VITA

Graduate School
Southern Illinois University

Bradley S. Sears [redacted]

PII Redacted [redacted]

Indiana University at Bloomington
Bachelor of Science Mathematics

Central Missouri State University
Master of Science, Applied Mathematics

Dissertation Title:

Two-Element Generation of Unitary Groups over Finite Fields

Major Professor: Andrew G. Earnest